CLAIMS

What is claimed is:

1. In a network access point, a method of processing encrypted communication, according to an encryption/decryption process, said method comprising;

receiving a first message from a wireless client, said first message comprising first values for a first random number and information identifying said wireless client and said access point and a first message authentication code of said information in said first message signed using a first signing key;

generating a second message comprising second values for a second random number and information identifying said access point and said wireless client and a second message authentication code of said information in said second message signed using a second signing key; and

sending said first values and said second values to an access point server, wherein said access point server generates a session key using said first and second values and third values provided by said access point server, such that said processing is shared by said access point and said access point server.

2. The method as recited in Claim 1 further comprising:

receiving a third message conveying said session key from said access point server, said third message having a first portion and a second portion; and

verifying said second portion of said third message against said second values.

3. The method as recited in Claim 1 further comprising:

sending said first portion of said third message to said wireless client, wherein said wireless client verifies said first portion of said third message against said first value, such that said session key is shared between said wireless client and said access point and said access point server.

4. The method as recited in Claim 2 wherein said first portion of said third message further comprises data for ensuring validity of said first portion and wherein said second portion of said third message further comprises data for ensuring validity of said second portion.

5. The method as recited in Claim 1 wherein said third value is correct for said encryption/decryption process.

6. The method as recited in Claim 1 wherein said network is a wireless network.

7. The method as recited in Claim 1 wherein said encrypting/decrypting process comprises a distributed symmetric key distribution process.

8. The method as recited in Claim 7 wherein said distributed symmetric key distribution process is Otway-Rees key cryptography.

9. A computer system in a computer system network, said computer system comprising:

a bus;

a memory unit coupled to said bus;

a processor coupled to said bus for executing a method of processing encrypted communication comprising:

receiving a first message from a wireless client, said first message comprising first values for a random number and information identifying said wireless client and an access point and a message authentication code of said information in said first message signed using a first signing key;

generating a second message comprising second values for a second random number and information identifying said access point and said wireless client and a message authentication code of said information in said second message signed using a second signing key; and

sending said first values and said second values to an access point server, wherein said access point server generates a session key using said first and second values and third values provided by said access point server, such that said processing is shared between said access point and said access point server.

10. The computer system of Claim 9 wherein said method further comprises:

receiving a third message conveying said session key from said access point server, said third message having a first portion and a second portion; and

verifying said second portion of third message against said second values.

11. The computer system of Claim 9 wherein said method further comprises:

sending said first portion of said third message to said wireless client, wherein said wireless client verifies said first portion of said third message key against said first value, such that said session key is shared between said wireless client and said access point and said access point server.

12. The computer system of Claim 10 wherein said first portion of said third message further comprises data for ensuring validity of said first portion and wherein said second portion of said third message further comprises data for ensuring validity of said second portion.

13. The computer system of Claim 9 wherein said third values are correct for said encryption/decryption process.

14. The computer system of Claim 9 wherein said network is a wireless network.

15. The computer system of Claim 9 wherein said encrypting/decrypting process comprises a distributed symmetric key distribution process.

16. The computer system of Claim 15 wherein said distributed symmetric key distribution process is Otway-Rees key cryptography.

17. A computer-usable medium having computer-readable program code embodied therein for causing a computer system to perform:

receiving a first message from a wireless client, said first message comprising first values for a random number and information identifying said wireless client and an access point and a message authentication code of said information in said first message signed using a first signing key;

generating a second message comprising second values for a second random number and information identifying said wireless client and said access point and a message authentication code of said information in said second message signed using a second signing key; and

sending said first values and said second values to an access point server, wherein said access point server generates a session key using said first and second values and third values provided by said access point server, such that processing of encrypted communication is shared between said access point and said access point server.

18. The computer-usable medium of Claim 17 wherein said computer-readable program code embodied therein causes a computer system to perform:

receiving a third message conveying said session key from said access point server, said third message having a first portion and a second portion; and

verifying said second portion of said third message against said second values.

19. The computer-usable medium of Claim 17 wherein said computer-readable program code embodied therein causes a computer system to perform:

sending said first portion of said third message to said wireless client, wherein said wireless client verifies said first portion of said third message against said first values, such that said session key is shared between said wireless client and said access point and said access point server.

20. The computer-usable medium of Claim 18 wherein said first portion of said third message further comprises data for ensuring validity of said first portion and wherein said second portion of said third message further comprises data for ensuring validity of said second portion.

21. The computer-usable medium of Claim 17 wherein said computer system is an access point in a network.

22. The computer-usable medium of Claim 21 wherein said third values are correct according to an encryption/decryption process implemented in said network.

23. The computer-usable medium of Claim 18 wherein said network is a wireless network.

24. The computer-usable medium of Claim 22 wherein said encryption/decryption process comprises a distributed symmetric key distribution process.

25. The computer-usable medium of Claim 24 wherein said distributed symmetric key distribution process is Otway-Rees key cryptography.